GeekBrains

Урок 5 Тема 2

Применение и обход антиотладочных приемов. Часть 1

Реверс-инжиниринг

В этом видео

1. Способы защиты от динамического анализа.
2. Признаки виртуального окружения.
3. Общие подходы к обходу антиотладочных приемов.
4. Способы обнаружения работы программы под отладчиком и их обход.

GeekBrains

Способы защиты от динамического анализа

- Обнаружение виртуальной машины:
    - выявление признаков виртуального окружения;
- Обнаружение отладчика:
    - замер времени выполнения;
    - контроль целостности кода;
    - специальные API операционной системы.

Признаки виртуального окружения

- Артефакты в реестре Windows:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services**Disk**\Enum
- Имена сетевых интерфейсов:
  - **VirtualBox** Host-Only Network
- MAC-адреса сетевых адаптеров:
  - **00-0C-29**-XX-XX-XX - VMware Inc.

Общие подходы к обходу антиотладочных приемов

- Устранение признаков обнаружения отладчика или виртуального окружения:
  - смена MAC-адреса;
  - смена имени сетевого интерфейса.
- Поиск места реализации проверки внутри программы и ее отключение:
  - замена инструкции CALL на несколько инструкций NOP;
  - замена инструкции JNZ на JZ.

Способы обнаружения работы программы под отладчиком

- **Измерение времени выполнения команд:**
  - **функция GetTickCount**
  - инструкция RDTSC
- Поиск отладочных артефактов:
  - процессы
  - окна
- Использование специальных API-функций ОС:
  - IsDebuggerPresent
  - CheckRemoteDebuggerPresent
  - NtQueryInformationProcess
- Контроль целостности кода.

GeekBrains

Способы обнаружения работы программы под отладчиком

- Измерение времени выполнения команд:
  - функция GetTickCount
  - инструкция RDTSC
- **Поиск отладочных артефактов:**
  - процессы
  - **окна**
- Использование специальных API-функций ОС:
  - IsDebuggerPresent
  - CheckRemoteDebuggerPresent
  - NtQueryInformationProcess
- Контроль целостности кода.

GeekBrains

Итоги

1. Познакомились с основными способами защиты от динамического анализа.
2. Узнали, по каким признакам можно обнаружить виртуальное окружение.
3. Увидели на практике, как работают некоторые способы защиты от динамического анализа.
4. Поняли, как рассмотренные способы защиты можно обойти.

GeekBrains